LA-UR- 96-3552

Title: LANSCE Personnel Access Control System (PACS)

Author(s): James C. Sturrock
Floyd R. Gallegos
Michael J. Hall

MASTER

Submitted to: Health Physics Society 1997 Midyear Topical Meeting
San Jose, CA

Los Alamos
NATIONAL LABORATORY

Form No. 836 R5
ST 2629 10/91

CONF-970134--14

LANSCE Personnel Access Control System *

James C. Sturrock, Floyd R. Gallegos, & Michael J. Hall

Los Alamos Neutron Science Center, AOT Division, Los Alamos National Laboratory, Los Alamos, NM 87545 USA

Abstract

The Radiation Security System (RSS) at the Los Alamos Neutron Science Center (LANSCE) provides personnel protection from prompt radiation due to accelerated beam. The Personnel Access Control System (PACS) is a component of the RSS that is designed to prevent personnel access to areas where prompt radiation is a hazard.

PACS was designed to replace several older personnel safety systems (PSS) with a single modern unified design. Lessons learned from the operation over the last 20 years were incorporated into a redundant sensor, single-point failure safe, fault tolerant, and tamper-resistant system that prevents access to the beam areas by controlling the access keys and beam stoppers. PACS uses a layered philosophy to the physical and electronic design. The most critical assemblies are battery backed up, relay logic circuits; less critical devices use Programmable Logic Controllers (PLCs) for timing functions and communications. Outside reviewers have reviewed the operational safety of the design.

The design philosophy, lessons learned, hardware design, software design, operation, and limitations of the device are described.

Introduction

The Personnel Access Control System (PACS) was designed as an integral part of an instrumentation-based, engineered personnel protection system: the Radiation Security System (RSS) at the Los Alamos Neutron Science Center (LANSCE). Other components of the RSS include fail-safe ion chamber systems, beam current limiters, safety system logic and wiring, and safety system beam transmission mitigation devices (beam plugs or stoppers). As part of this system PACS controls personnel access to areas that have radiological (prompt radiation) hazards when the LANSCE beam delivery system is in operation. It also provides a hardware means of enforcing administrative requirements during pre-operational sweeps of the exclusion areas.

The major drivers for the development of PACS were the compliance requirements of "DOE Order 5480.25, Safety of Accelerator Facilities", "Guidance for DOE Order 5480.25, Safety of Accelerator Facilities", and the LANL requirement to meet the provisions of Los Alamos Laboratory Standard "LS107-01.1, Accelerator Access-Control Systems". In addition, the LANSCE beam delivery system has evolved over 20 years with a variety of access control systems. These forces culminated in the design and gradual implementation of PACS across the entire LANSCE beam delivery system. An outside review panel was convened to ensure that

* Work supported by the U. S. Department of Energy

DISCLAIMER

PACS met the requirements of DOE 5480.25 and LS 107-01.1. The panel agreed that the requirements were met and made some suggestions to improve the reliability of the overall system.

Design Philosophy

PACS is designed to be a "fail-safe" access control system. "Fail-safe" is defined, for an area in the "Secure" state, to mean functioning as intended or in the event of a single component failure, the system will either function as intended (due to redundant circuitry) or will revert to an "Open" state and prevent delivery of the beam to the area. PACS is also designed to be fault tolerant. This allows the system to operate correctly in some degraded situations, but to alarm the operators that there is a problem.

Entry is limited by barriers with entry points (doors). Redundant limit switches on doors detect breech of access point or secure state of door. Sweep of the area is performed by a team and uses a loop of reset switches as a sweep confirmation. Access through the doors is controlled by a Kirk key entry lock system. SCRAM switches are available inside the exclusion area. The SCRAM switches and barrier limit switches are connected in a loop.

Design Requirements, General Specifications, and Implementation Details

Refer to Fig. 1 for functional block information.

- Personnel access is controlled to areas by locked physical barriers. All lock cylinder cores to be compatible with ABB Kirk key control hardware.
- Self-checking circuitry and fail-safe design of sensor wiring. The implementation of the sensor wiring uses redundant loops run in the same cable. To prevent crossed wiring from potentially bypassing a sensor, the two loops are run with opposite polarity 24 volts. Ground fault sensing relays indicate any crossed loop wiring. This condition will not normally shut the system down, but will indicate a fault that must be corrected before the system is placed in a "Secure" state again. To prevent a wiring fault from bypassing a sensor, the incoming and outgoing wires from each sensor are routed through different paths and the completed sensor wiring forms a loop with separate inputs and outputs to the sensitive wiring panel in the Main Access Control Panel (MACP).
- Self-checking and tamper resistant reset loop. The reset loop switches and relays are all checked before each sweep to ensure that they are not closed. In addition, the reset input to the MACP is checked to see that it is not made up before the sweep occurs. These features add confidence that the reset loops are operating properly prior to a sweep operation. The reset switches use light emitting diodes (LEDs) to direct the sweep and to report the status of each reset. The next reset switch to be activated shows a green LED and when the switch has been pushed, the green LED goes out and a yellow LED comes on.
- Self-directing (indicate flow and status of the personnel sweep) control panels both at the Remote Access Control Panel (RACP) and at the MACP. The indicator panels at both stations show the progress of the sweep and direct what step is to be taken next.

- Modular construction of the equipment which allows rapid replacement of line replaceable units (LRU) to minimize down time for servicing. Ability to change most of the LRUs with the system in a "Secure" state and the power "On". Every LRU in the MACP, with the exception of the sensitive wiring board and the Access Control Module (ACM), can be removed from the enclosure and replaced without dropping a "Secure" state or losing the ability to monitor the sensor loops for breaks.

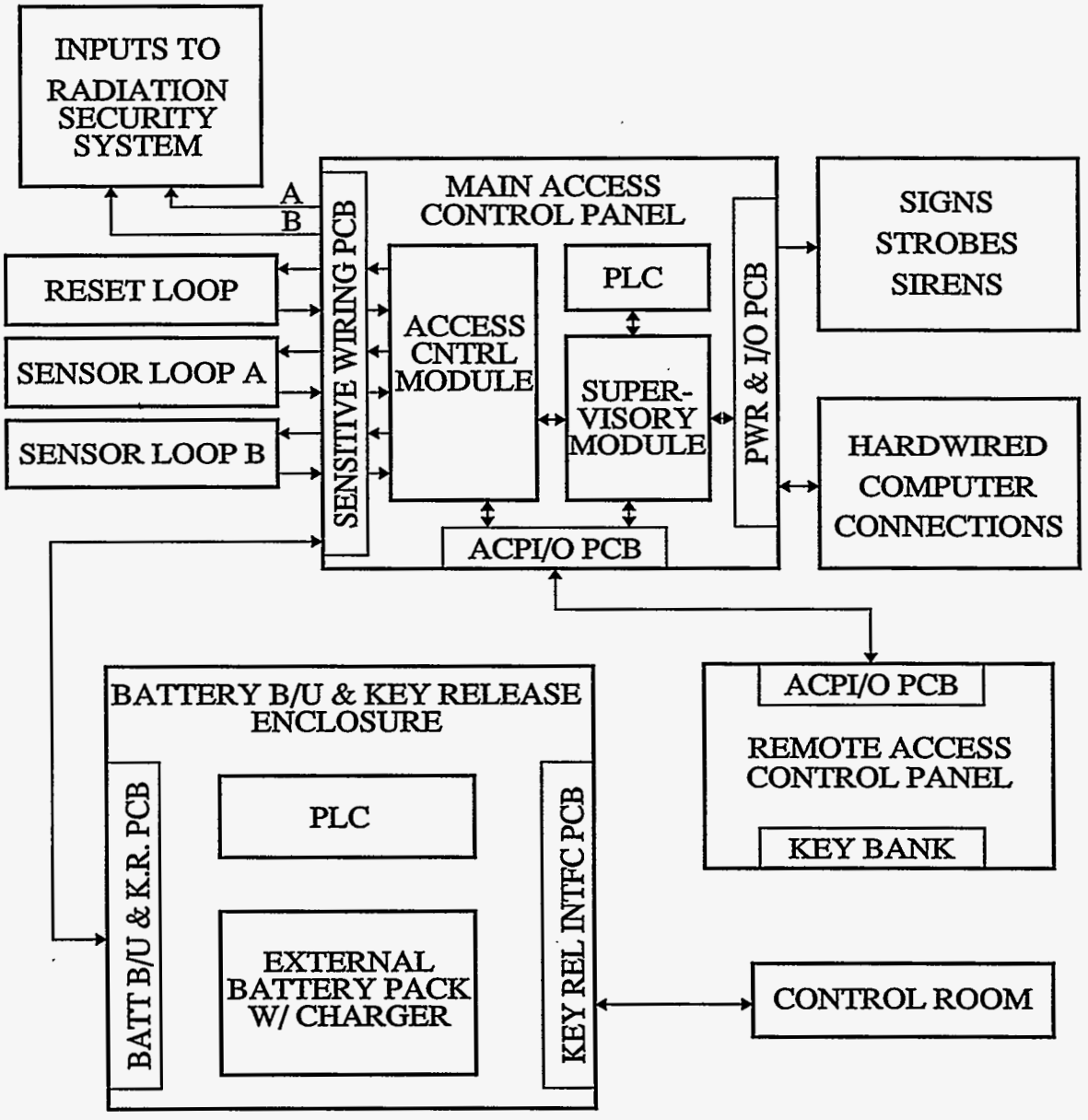

FIGURE 1. Block diagram of the LANSCE Personnel Access Control System (PACS)

- Layered approach to the system construction, i.e., in the MACP, the outside of the box allows general access to the system indication and reset functions, a simple lock allows access to the PLC (Programmable Logic Controller) and the Supervisory Module (SM), and an RSS padlock allows access by the RSS engineer or his designee to the bottom level where the wiring interfaces and ACM are located.
- Battery backed up "Secure" state to prevent having to resweep in the event of a power failure. Centrally located batteries supply the PACS and if the system is in a "Secure" state when power fails, the batteries keep the systems in a "Secure" state and active. If the system is not in a "Secure" state when the power fails, it will remain dead until power is reapplied and the personnel sweep resets the system to a "Secure" state.
- A distributed battery backup and key release system with nodes located in central areas. The battery back up and key release nodes also receive information from beam-plug in-limit sensors and other devices which are part of system "safe circuitry" and process the data with a PLC to generate access "ready" conditions for the operators. When this "key release allowed" status is received in the control room, the operator pushes a key release switch on the console which then lights an "Access Allowed" indicator on the RACP. The person at the RACP then pushes the key release switch and removes the released key. In emergency situations there is a mechanical, key-controlled override that allows access to exclusion areas. PACS reverts to an "Open" state if the emergency-override is used.

Device Descriptions

Refer to Fig. 2 for an actual installation of a PACS entry station that shows many of the components listed below.

Scram switches: These sensor loop devices are mounted in a 4-inch cubic cast aluminum box with a large mushroom actuator that is brightly illuminated by an LED lamp. When the actuator is pushed, it latches in the closed position and the LED is extinguished. Used as the primary beam line panic sensor.

Door monitor and exit door monitor: Both door monitor sensor loop devices are mounted in a 4-inch cubic cast aluminum box with two LED indicators that show the status of the monitored door switches. The exit door monitor allows the door to be bypassed during the time that the sweep team is exiting the area.

Door sensor switches: Door sensor loop devices are mounted in a 3-inch by 4-inch by 8-inch aluminum box mounted above the door to be sensed. A contoured probe is attached to the door and enters the sensor switch box and actuates switches. The switches are arranged in four independent sets where the first is an anti-tamper switch and the last is the actual loop or indicator sensor. Each loop has a loop sensor and an indicator sensor. In addition there can be two complete sets of switches for use in dual exclusion area situations.

Bypass switches: Bypass sensor loop devices are mounted in a 4-inch by 8-inch by 4-inch cast aluminum box and are key-controlled door bypass switches to be used when it is necessary to sweep an area with a barrier in the open position. An example of this condition would be a target cell where the shield door takes 10 minutes to close and occupation of the area with the door shut is not allowed for emergency egress reasons.

Reset switches: Reset loop devices are mounted in a 4-inch cubic cast aluminum box with a push button reset switch and two LED indicators. There are two kinds of reset devices, one is for sequential reset and the other for random reset. In either case, the green LED is illuminated when the reset is the next one that needs to be swept. The yellow LED indicates that the reset has been swept and accepted by the system. The last reset switch by the exit door enables an exit door bypass that is timer controlled by the PLC in the main electronics enclosure.

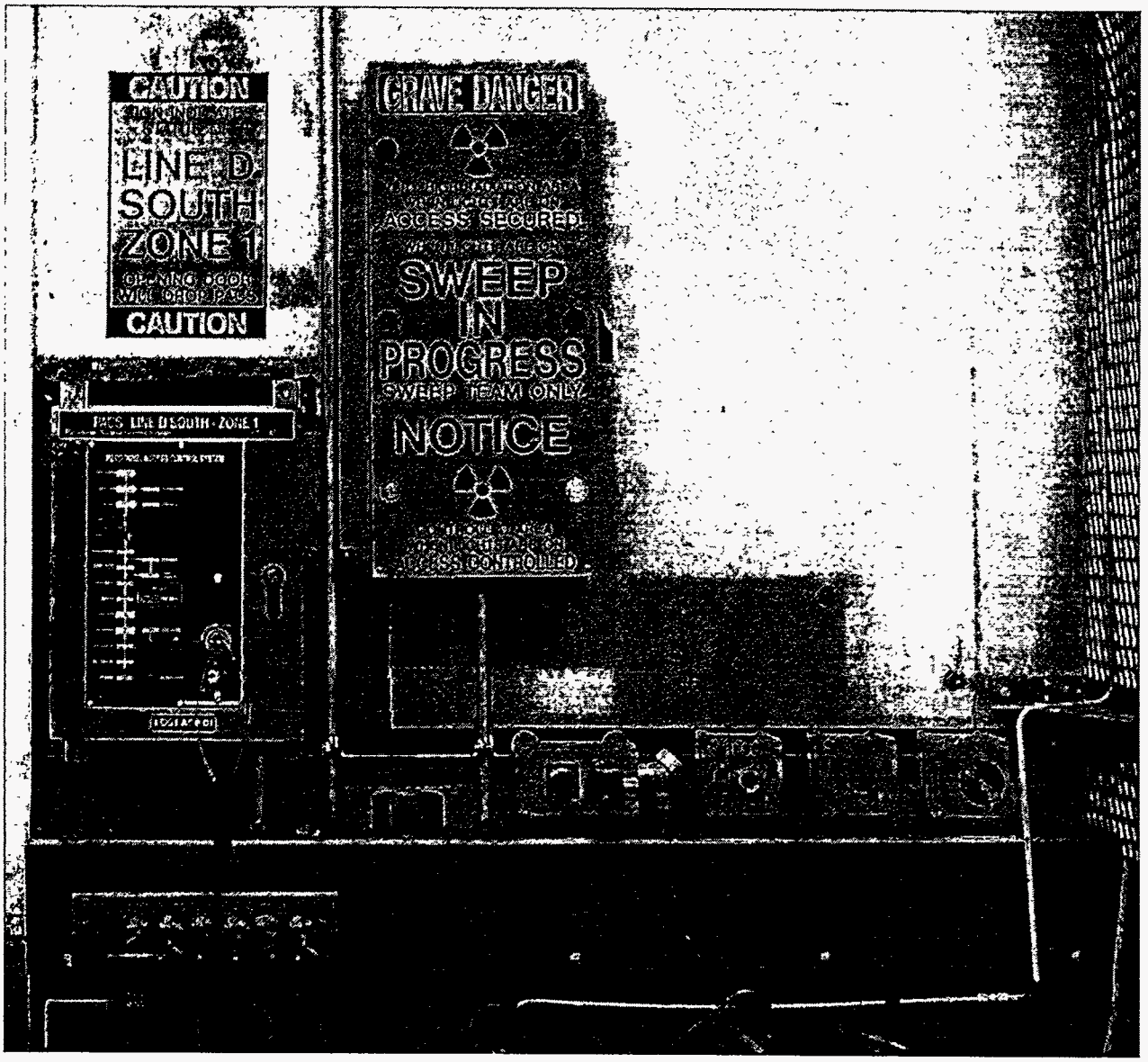

FIGURE 2. Actual PACS installation in Line D South of the LANSCE Beam Delivery System. Components shown (from left to right) Remote Access Control Panel (RACP) including the Kirk key capture and release mechanism, sign assembly, shield door bypass switch, Reset switch, Door monitor, SCRAM switch, and (in the lower left) a Kirk key transfer bank.

Signs, strobe and siren assemblies: Signs in various configurations (i.e., flat sign displays, angled sign displays, and with or without sirens and strobes) are distributed throughout the exclusion area and at the entrance to the exclusion area.

Main access control panel (MACP): The MACP is a 24-inch square by 12-inch box with a clear cover housing all of the electronics for the PACS. It is normally mounted in a benign environment and only needs to be visited to reset system faults. The MACP is divided into three levels with varying degrees of security. The uppermost level is outside the enclosure and allows access to the Access Display Panel (ADP), system reset switch, panel LED test button. Viewing of the PLC with its display and the SM with its Electronics and Display PCB (EAD), is also allowed at this level. A simple maintenance lock allows access to the PLC and the SM. The most secure area in the MACP is the lower level and it is controlled by an RSS padlock. The key to this lock is controlled by the RSS Engineer and must be signed out from the control room with permission of the RSS Engineer. The lower level contains all of the system wiring interface, the ACM, and the system power supplies.

Hardwired output connections: The output connections primarily go to the operations computer where they are sent to the control room as data.

Inputs to the Radiation Security System (RSS): The inputs to the RSS are separate dry contacts from the loop latching relays in the A and B sensor loops. These are the primary contacts that shut the accelerator beam off if the exclusion area is not in a "Secure" state. There are built in provisions to test these relays and their outputs separately to verify the operation of the PACS and RSS.

Remote access control panel (RACP): The RACP is a 12-inch by 16-inch by 6-inch panel with a clear cover housing the slave ADP and , if used, the Kirk key capture and release mechanism. An MACP can be used in place of an RACP when conditions permit.

Battery backup and key release enclosure: The battery backup and key release system is enclosed in a 30-inch square by 12-inch box with a clear cover. The battery system includes the battery charge, direct current distribution system , and the batteries themselves which are mounted in a separate enclosure on the floor. The key release system includes inputs from the beam plugs or other beam control devices, outputs to and inputs from the control room, outputs to the various key-controlled areas, and a PLC to handle the key-release logic. The entire key-release system is powered from the backup battery to provide access capability in the event of a power outage. The rational behind the key-release logic is to prevent challenges to the RSS and to prevent unexpected shut down of the LANSCE beam delivery system. It prevents the control room operator from issuing a key-release command until the beam delivery system has been shut down and not relying on the PACS to shut the beam delivery system down when it goes into an "Open" state.

Operation

System operation will be explained by a walk through of a typical exclusion area by two operations personnel who enter and then secure the PACS. The entry station contains an RACP, a flat three panel sign (with three placards, the top most is the secure radiation classification sign and is indicated with red LEDs, the middle sign is for sweep in progress and is indicated by yellow LEDs, and the lower sign is the open radiation classification sign and is indicated with green LEDs), an exit door monitor, a Kirk key bank and an intercom station. The operators

follow the procedure contained in the "Operations Manual" for the particular area and use the intercom to call the control room and request a key release. The control room personnel ensure that the beam delivery system is safe. When the key release logic is ready and the control room operator push the key release switch, a key release command is issued to the area. The operator at the entry station must then press the key release switch on the RACP at the same time that the key release command is issued by the control room. The logic contained in the MACP forces the system into an "Open" state and then operates a solenoid in the key capture device to release the key-bank transfer key. The transfer key is inserted into the key-bank and turned in order to release the door keys. Each person making an entry takes a door key and proceeds to enter the exclusion area. In an emergency, a purely mechanical means allows an emergency key, which is available in the control room, to release the key-bank transfer key. If the system is entered by any means other than a normal key release from the control room, a system fault is generated and latched into the Supervisory Module (SM) as a loop-break fault.

When it is time to secure the area, the operators follow the procedure contained in the "Operations Manual" and proceed to start a personnel sweep of the area. All system faults must be cleared in order to go into the "Sweep In Progress" mode. If a fault occurs at any time during the sweep, then the sweep is terminated and the fault must be cleared before it can be started again. The system is placed into a "Sweep In Progress" mode by pushing the switch on the RACP. When the sweep-in-progress switch is pushed, the system automatically sounds the sirens and operates the strobe lights for thirty seconds. When the sirens stop, an announcement is made, by the personnel performing the sweep, to clear the area. The sweep team takes the rest of the keys from the key-bank, check to see that the two sensor loops are made up (indicators on the RACP) and enter the area ,making sure to close the exit door behind themselves. If any door or barrier is operated during the sweep, the sweep must start over at the first reset station. This prevents any unexpected intrusion into the area during a sweep. The operators proceed to the first reset station, which will have its green LED illuminated to indicate that it is ready to be reset (if the sensors loops are not made up, this green LED will not be illuminated), and press the reset switch. The green LED goes out and the yellow LED comes on to indicate that the station is reset. The operators check the area carefully to make certain that no one is swept in and proceed to the next reset station. Each door or other barrier in the area has its own door monitor. These monitors have two green LEDs on them that indicate the status of the two loop sensors that monitor the door. Both sensors must be in the closed position for the sweep to start and the green LEDs furnish feedback to the operators that the two loops are complete. When the last reset station is swept, a timer starts that bypasses the exit door for thirty seconds. The sweep team must leave the area before the bypass times out or they will have to resweep the area. Once the sweep team has left the exclusion area, they must return the keys to the key-bank and release the transfer key which is then placed into the key capture device on the RACP. When this key is captured, the system automatically sounds the sirens and flashes the strobes. The sweep team make an announcement stating that the area is secure and after thirty seconds, the logic in the MACP forces the system into a "Secure" state. The "Sweep In Progress" mode may also be terminated when the sweep off switch is pushed on the RACP.

In the event of a power outage while the system is in a "Secure" state, the logic in the Access Control Module in the MACP automatically switches over to the backup battery. The system

will stay in the "Secure" state and will continue to monitor the two sensor loops. If a loop is broken, the system reverts to an "Open" state. The system can not be placed into a "Secure" state during a power outage. The key-release system is active during a power outage and following the procedure above, a key release command can be given by the control room and the transfer key released. The battery backup is designed to provide a minimum of 8 hours of operation for the entire system.

The A and B sensor loops are totally independent of each other and are physically arranged so that it is most unlikely that the sensor can be defeated. All sensor loop wiring enters on one side of a sensor and exits through the other. The loop sensor wires are color coded and there are no spare wiring terminals. The A loop is powered by a plus twenty four volt source and the B loop is powered by a minus twenty four volt source. The sensor loop relays are returned to the other side of their respective power sources and these two points are connected to earth ground through ground fault sensing circuitry. If the loops are crossed, the ground fault sensing circuitry operates and latches a fault on the Supervisory Module (SM). There are also low voltage sensors on the loop voltages and if the voltage drops below approximately 18 volts, a fault is latched on the SM. If the system is in a "Secure" state, a ground fault or minor low voltage will not force the system into an "Open" state. If the voltage drops too low, the relays will drop out and the system will revert to an "Open" state. The sensors used in the loops are all switches. The door sensors are special switch assemblies that mate with a contoured probe to provide a level of tamper resistance. Special cases such as roll-up doors or kick panels can be sensed with high quality enclosed industrial switch assemblies. Indoor fences, shield blocks and other physical items that must be present to make up the shielding barrier integrity can be monitored by simply passing loops of insulated wire through them such that if the barrier is moved, the wire will be broken. Outdoor fences, shield blocks, etc. require extensive lightning protection. We are investigating several non-electrical means such as a fiber optic or pneumatic loop sensors that would close contacts in the A and B sensor loops. The sensor loops are executed entirely in relay logic. The relays chosen for this job are extremely reliable four pole normally open relays. One pole of each of these relays is the contact that goes to the RSS, one pole is used to latch the relay, one pole is used to fan the relay out for other functions and the last pole is used for the output relay test function.

The reset loop is arranged to force the sweep into all areas where a person could be overlooked. This includes all dead ends, alcoves and other areas where a person could be working or in the worst case passed out and lying on the floor. There are two kinds of reset stations: one is for sequential sweeps and the other is for random sweeps. The sequential is the most widely used, since it forces a definite pattern to the sweep. The reset circuitry has a number of self-checking and anti-tamper features built into it. During the period when the initial horn is being blown, the reset circuit checks to see that there are no switches pushed and that none of the latching reset relays are closed. If either case exists, a fault is latched that must be cleared before the sweep can proceed. The other condition verifies that the reset loop has not been bypassed. This also sets a fault that must be cleared before the sweep can be resumed.

Programmable Logic Controllers (PLCs) in PACS are used in the MACP to direct the sweep, to provide time delays and to report information back to the control room computers. The only

PLC interaction with the sensor loops is to issue the command to latch the loops when the sweep is complete. This latching circuit is carefully protected from any false latching signal by relay contacts from the fault string, keys returned logic and reset OK logic. Furthermore it is protected from a continuous 24 VDC level by blocking capacitors.

The PLC in the battery backup and key release enclosure is used to verify that the beam plugs and stoppers are in the correct configuration for safe entry into an area.

Vulnerabilities

Indicators and electronics are vulnerable to radiation damage. The green LEDs used on the signs and the LEDs in the RACP tend to dim upon exposure to intense radiation. This effect is quite noticeable for exposures above a few hundred Rad. The strobe electronics contain a trigger device that fails after exposure to a few hundred Rad. A solution to the LED problem is to use incandescent lamps. This has its own set of problems, but it appears to be a better solution in areas of intense radiation. The strobe trigger was replaced with a spark gap device and is undergoing evaluation.

The ground fault detector used in the sensor loops is quite sensitive. It has faulted numerous times during wet weather when mist blows into the door sensor. It does detect real problems with water leakage into the sensors, but it also is somewhat sensitive to normal conditions like an open door in the rain. A plastic flap is being tested to help prevent water infiltration into the sensor assembly.

Summary

The ten PACS installations have been in service for four months with no system failures. There have been a number of faults reported by the system that indicated sensor loop ground faults and power outages. There have been no cases of a system in the "Secure" state being dropped to an "Open" state during a power outage or any abnormal loss of "Secure" state by a PACS device.

Minor upgrades are being implemented to the system in the next year and another seven PACS installations are planned for the middle of the coming year. This will finish the main LANSCE beam delivery system installation of PACS. In the future the system will be installed in experimental beam lines and in other portions of the of the LANSCE accelerator complex.

Acknowledgments

The authors are indebted to the LANSCE Beam Delivery Team and the other subject matter experts in AOT Division for their advice in the development and implementation of the complex Personnel Access Control System (PACS). Their input to the process enabled the final result to perform properly and to be acceptable to end users.